ABSTRACT OF THE DISCLOSURE

A method and system for encrypting and decrypting a message. A message is created by appending an error detection code to an information block. The binary value of the resulting message is then compared to the sender's encryption

5   modulus. If the binary value of the message is greater than or equal to the sender's encryption modulus, at least one bit of the error detection code is altered to reduce the binary value of the message below the sender's encryption modulus. The potentially modified message is then encrypted once using the sender's private key to generate a once encrypted message referred to herein as the signed message.

10 The signed message is then encrypted using the recipient's public key to produce a doubly encrypted bitstring. The recipient deciphers and decodes the doubly encrypted bitstring. If an decoding failure occurs, the recipient assumes that the error is due to an intentional bit change by the sender and attempts to restore the presumably altered bit or bits to their presumed original value.